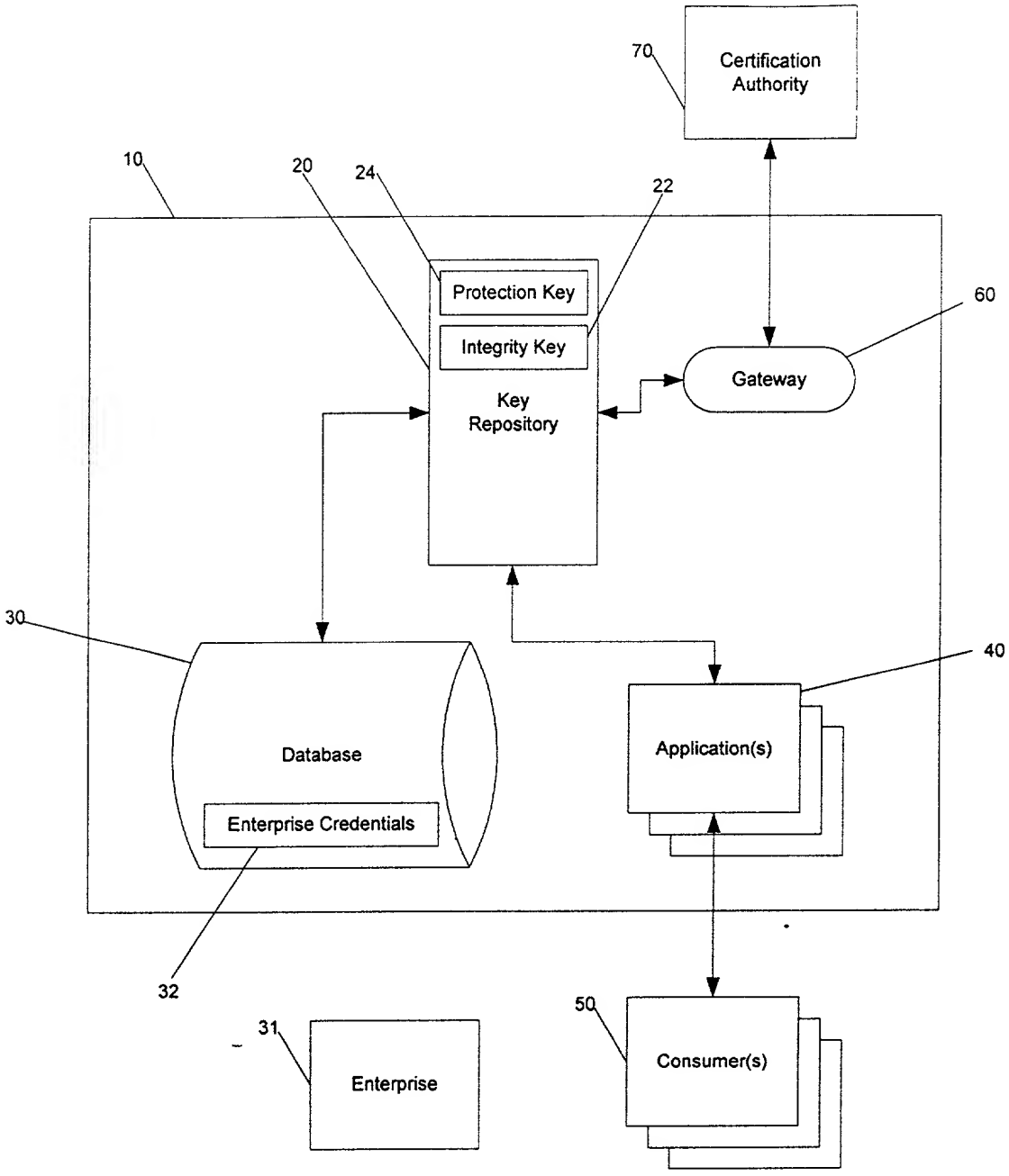
70
Certification Authority
10
20
24
22
Protection Key
Integrity Key
Key Repository
60
Gateway
30
Database
Enterprise Credentials
40
Application(s)
32
31
Enterprise
50
Consumer(s)

Figure 1

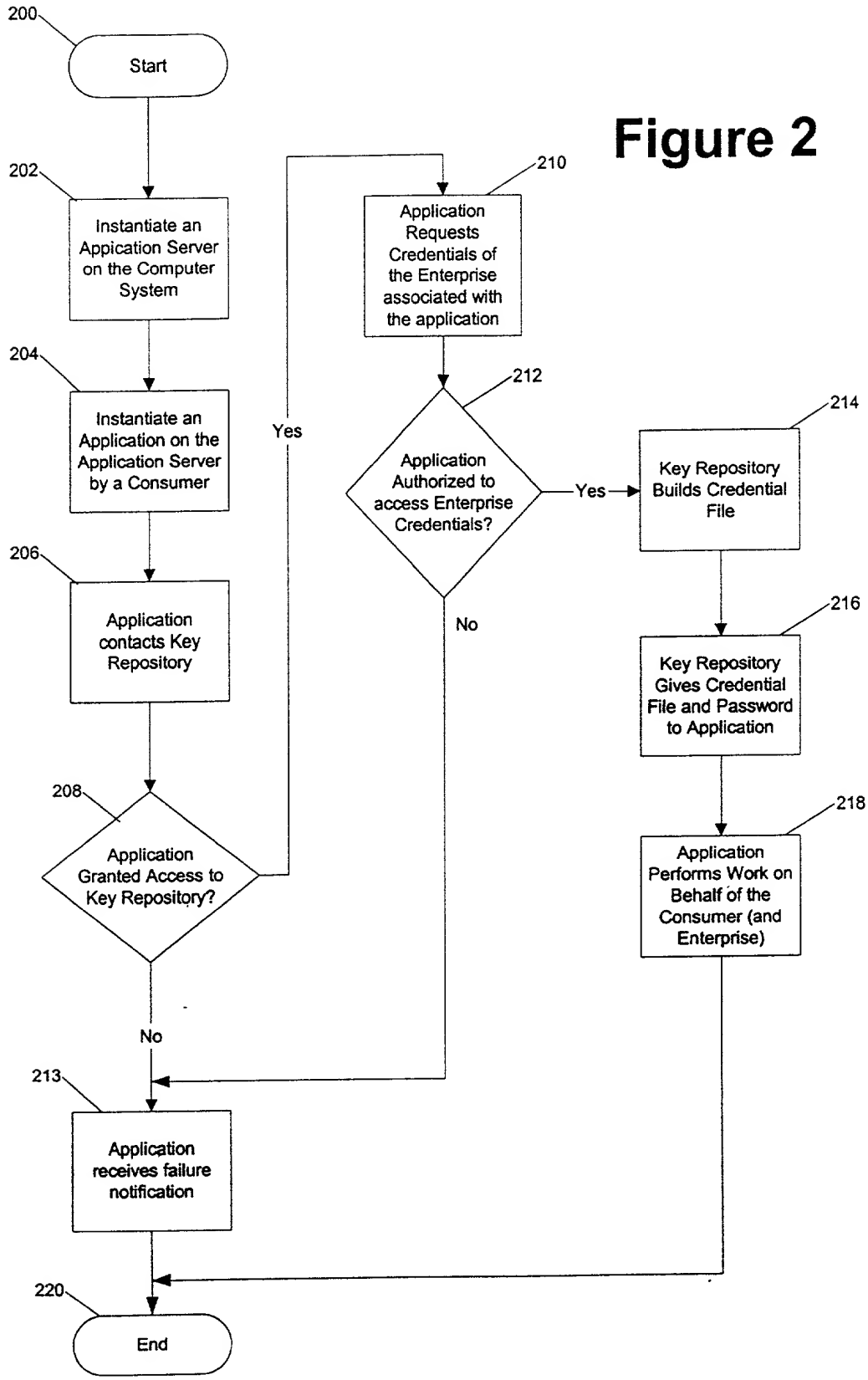
200
Start
202
Instantiate an Appication Server on the Computer System
204
Instantiate an Application on the Application Server by a Consumer
206
Application contacts Key Repository
208
Application Granted Access to Key Repository?
Yes
No
210
Application Requests Credentials of the Enterprise associated with the application
212
Application Authorized to access Enterprise Credentials?
Yes
No
214
Key Repository Builds Credential File
216
Key Repository Gives Credential File and Password to Application
218
Application Performs Work on Behalf of the Consumer (and Enterprise)
213
Application receives failure notification
220
End

Figure 2

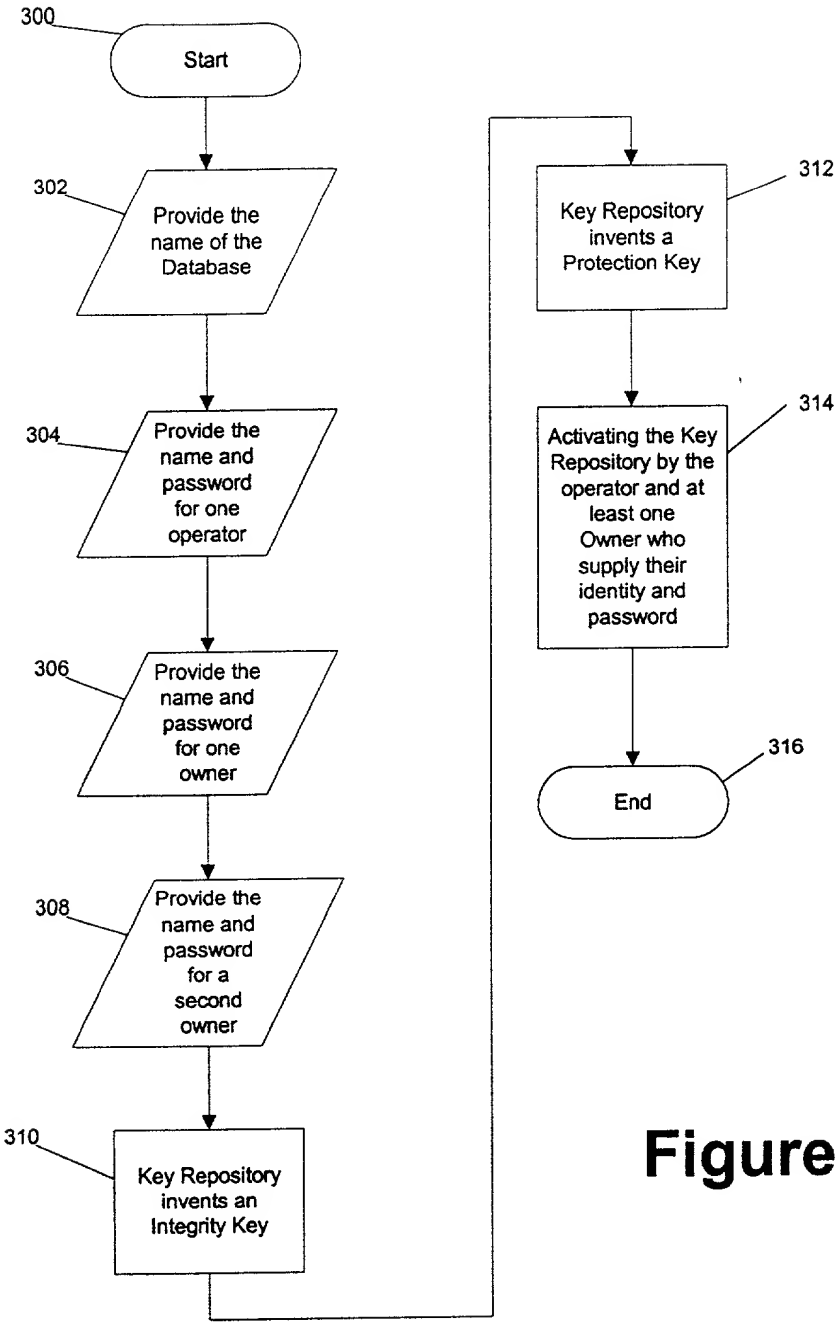
300
Start
302
Provide the name of the Database
304
Provide the name and password for one operator
306
Provide the name and password for one owner
308
Provide the name and password for a second owner
310
Key Repository invents an Integrity Key
312
Key Repository invents a Protection Key
314
Activating the Key Repository by the operator and at least one Owner who supply their identity and password
316
End

Figure 3

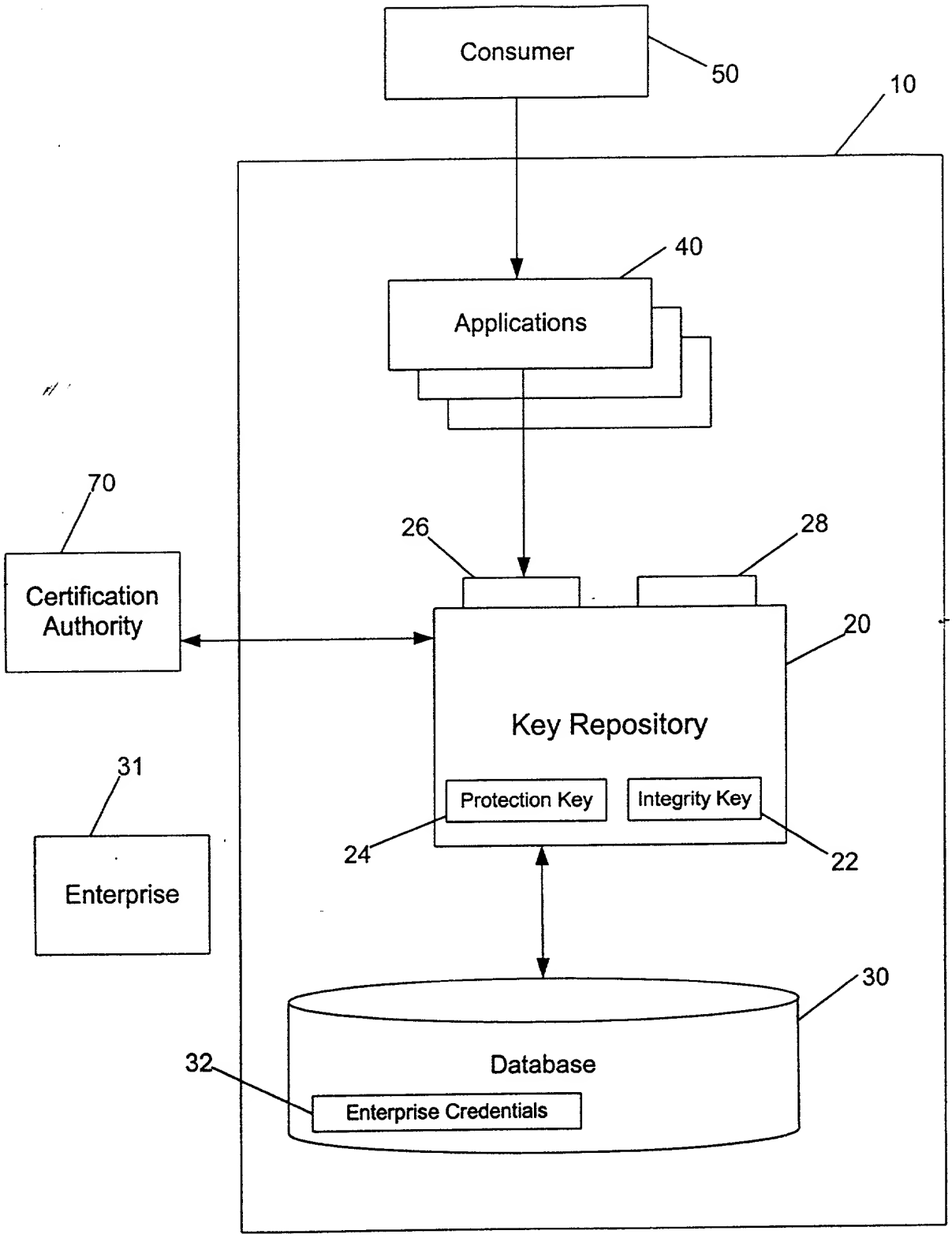
Consumer
50
10
40
Applications
70
Certification Authority
26
28
20
Key Repository
Protection Key
Integrity Key
24
22
31
Enterprise
30
Database
32
Enterprise Credentials

Figure 4

Docket No. 3768.5

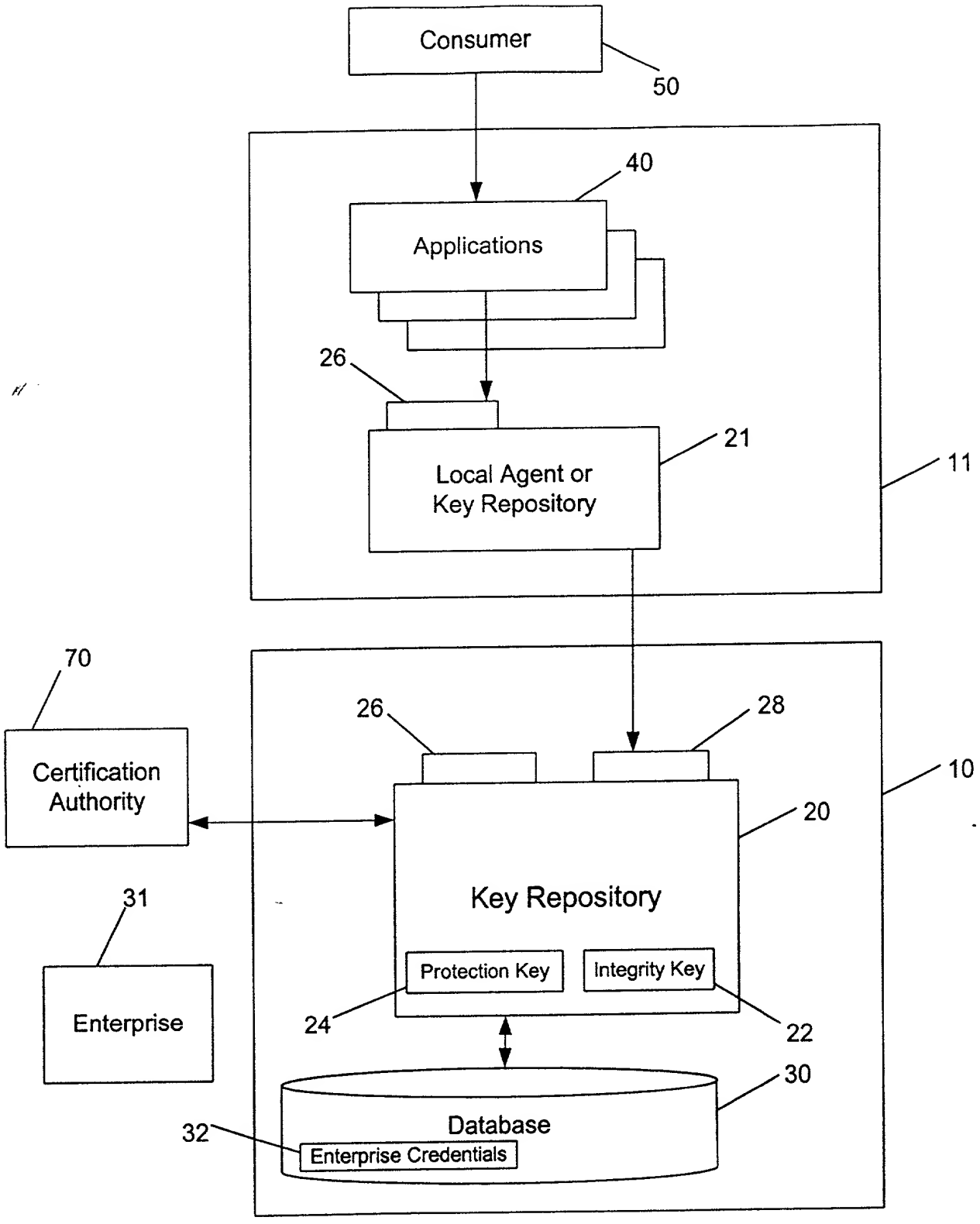

Figure 5

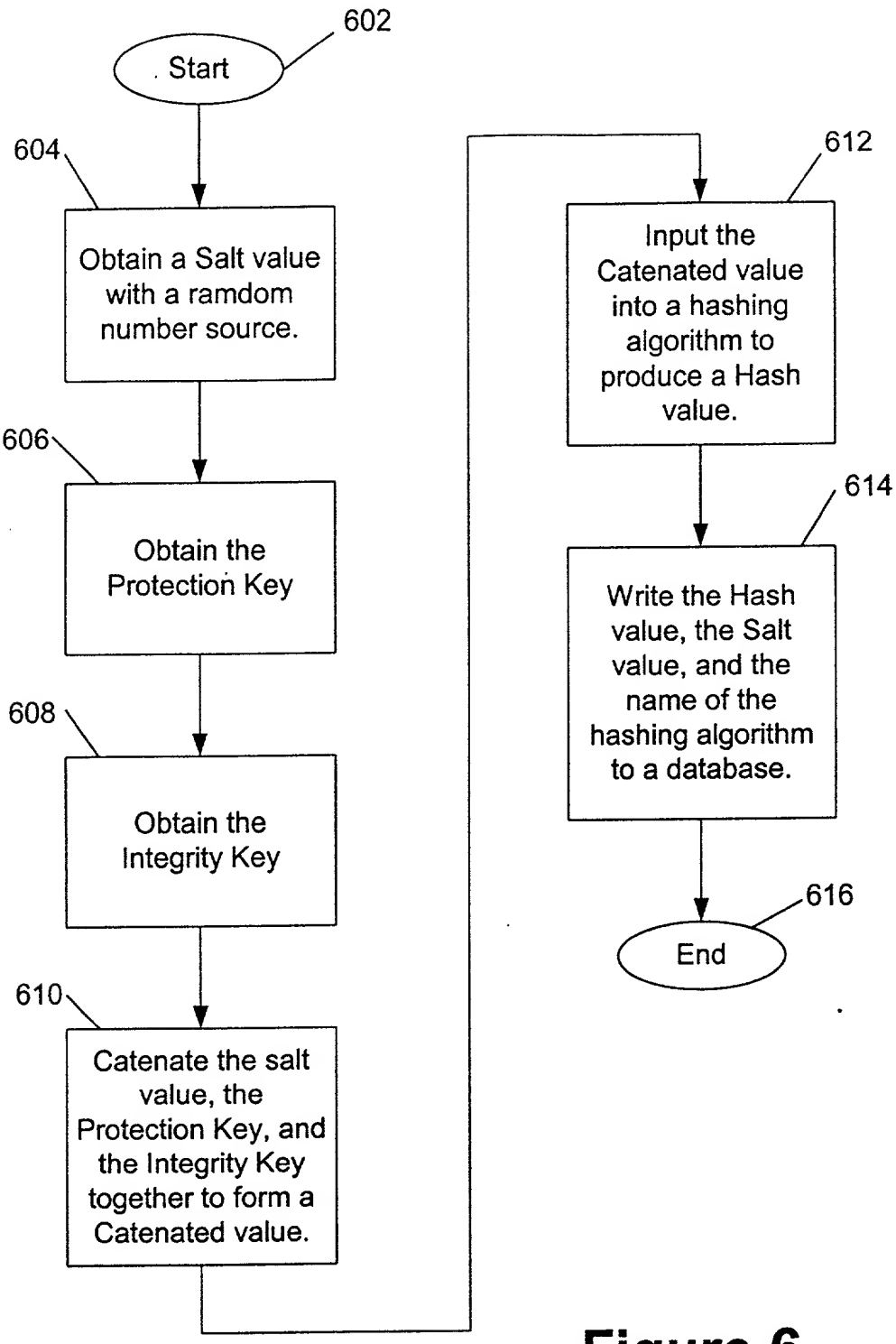
602
Start
604
Obtain a Salt value with a ramdom number source.
606
Obtain the Protection Key
608
Obtain the Integrity Key
610
Catenate the salt value, the Protection Key, and the Integrity Key together to form a Catenated value.
612
Input the Catenated value into a hashing algorithm to produce a Hash value.
614
Write the Hash value, the Salt value, and the name of the hashing algorithm to a database.
616
End

Figure 6